AF 2635

TRANSMITTAL OF APPEAL BRIEF (Large Entity)	Docket No. ITL.0781US

In Re Application Of: **ANIMESH MISHRA, ET AL.**

#12 / Appeal Brief

Serial No.	Filing Date	Examiner	Group Art Unit
09/765,823	January 19, 2001	Edwin C. Holloway, III	2635

1/28/04

Invention: **THEFT PREVENTION USING LOCATION DETERMINATION**

TO THE COMMISSIONER FOR PATENTS:

Transmitted herewith in triplicate is the Appeal Brief in this application, with respect to the Notice of Appeal filed on

The fee for filing this Appeal Brief is: **$330.00**

☒ A check in the amount of the fee is enclosed.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. **20-1504**

Signature

Dated: **January 15, 2004**

John A. Odozynski, Reg. No. 28,769
TROP, PRUNER & HU, P.C.
8554 Katy Freeway, Suite 100
Houston, TX 77024

I certify that this document and fee is being deposited on **January 15, 2004** with the U.S. Postal Service as first class mail under 37 C.F.R. 1.8 and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signature of Person Mailing Correspondence

Jennifer Juarez

Typed or Printed Name of Person Mailing Correspondence

cc:

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	ANIMESH MISHRA, ET AL.	Group Art Unit:	2635
Serial No.:	09/765,823	Examiner:	Edwin C. Holloway, III
Filed:	January 19, 2001		
For:	THEFT PREVENTION USING LOCATION DETERMINATION	Atty. Dkt. No.:	ITL.0781US (P10482)

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

This Appeal Brief is submitted, in accordance with the Notice of Appeal mailed December 31, 2003, by the Appellants to the Board of Patent Appeals and Interferences. Appeal is hereby taken from the final rejection of Claims 1-20 and 31-73, that rejection rendered in Paper No. 10, mailed October 6, 2003 ("the Final Office Action").

I. REAL PARTY IN INTEREST

The real party in interest is the assignee Intel Corporation.

II. RELATED APPEALS AND INTERFERENCES

None.

III. STATUS OF THE CLAIMS

Claims 1-3, 6-9, 11-20, 31-45 and 47-73 stand rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 5,532,690, *Apparatus and Method For Monitoring and*

Bounding the Path of a Ground Vehicle ("Hertel"), in view of U.S. Patent No. 5,557,254, *Programmable Vehicle Monitoring and Security System Having Multiple Access Verification Devices* ("Johnson, et al.")

Claims 4, 5, 10 and 46 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Hertel and Johnson, et al., in combination with U.S. Patent No. 5,223,844, *Vehicle Tracking and Security System* ("Mansell").

IV. STATUS OF AMENDMENTS

All Amendments previously presented by the Appellant have been entered as of the date of this Appeal.

V. SUMMARY OF THE INVENTION

FIG. 1 illustrates a system 10 according to this invention, including an exemplary device 12 to be protected against theft. For simplicity, the device 12 will be referred to as an appliance, but it is to be understood that device 12 may be any type of device whatsoever, such as an automobile, a home appliance, a computer, or a television.

The appliance is coupled over a communication link to a central agency 16 service or device which may, in turn, be coupled over a notification link 18 to a law enforcement agency device 20, such as a central dispatch computer, radio, or the like. The communication link and the notification link may utilize a telephone network, computer network, the internet, wireless, cellular, satellite, laser, audio, or any other suitable mechanism.

The appliance includes a local policy enforcer 30, a location determiner 32, which may be a location determination device or a motion detection device, a user authenticator 34, an appliance disabler/enabler, a functional unit 38, and a communication interface 39.

The local policy enforcer may constitute a software-programmed microprocessor, hard-wired logic, or other suitable means of performing the functionality of the local policy enforcer, which will be described below.

The location determiner may be a rudimentary device, such as simplistic as a mercury switch, which detects only motion but not relative position much less absolute position. It may be a more complex device such as a GPS receiver, which detects absolute position as well as motion; or it may be something in between such as an accelerometer, which detects motion and relative position but not absolute position.

The user authenticator may be as simple as a key device which may readily be possessed by any user; or it may be as complex as a biometric identity analyzer which is specific to a single individual user; or it may be something in between such as a password system. It may include simply a data gathering mechanism, but it may also include means for applying policies or comparing the data against, for example, a locally-stored copy of known-valid data, such as from a previously sampled user input.

The enabler/disabler is adapted for enabling and/or disabling the functional unit. In some embodiments, the functional unit may be in a default state of disablement until the enabler/disabler enables it. In other embodiments, the functional unit may be enabled unless the enabler/disabler disables it.

The functional unit provides the functionality of the appliance and would typically be found in an appliance which lacks the features of this invention; for example, in the case of a television, the functional unit might be the tuner or the display or the on/off switch.

The appliance's communication interface is suitably adapted for communicating over the chosen communication link. In one embodiment, the location determiner and user authenticator

may be coupled to the local policy enforcer, and the local policy enforcer may be coupled to the communication interface. Other configurations will, of course, be apparent given the teachings of this patent.

The central agency service or device 16 includes a communication interface 44 which is suitably adapted for communicating with the appliance over the communication link. It further includes a remote policy enforcer 40, an appliance registry 42, an optional user authenticator 43, and an optional notification interface 46. The remote policy enforcer may constitute a software-programmed microprocessor, hard-wired logic, or other suitable means of performing the functionality of the remote policy enforcer, which will be described below. The appliance registry may include a database or other suitable data storage and retrieval system, and a storage device for housing the database, such as a hard disk, a tape drive, a DVD-R drive, semiconductor memory, or other suitable storage means. The user authenticator 43 will not typically include a user data input gathering device, such as the biometric apparatus or password input means of the user authenticator 34 of the appliance. The central agency's user authenticator 43 may gather data through such user data input gathering device, and apply locally-held knowledge or policies, such as by comparing the user's biometric information against a stored database (not shown). The notification interface is suitably adapted for communicating over the chosen notification link.

FIG. 2 shows a flowchart which illustrates one exemplary embodiment of a method of operating the appliance of FIG. 1. FIG. 2 should also be understood to represent one or more information storage devices having stored thereon instructions, operations, routines, control codes, or the like, which, when loaded into or executed upon a programmed computer device, a programmable logic device, or the like, will cause such device to execute the exemplary method.

The method begins (59) with the appliance being disabled (60). The appliance determines (61), via its location determiner, where the appliance is presently located. In the rudimentary case of e.g. a mercury switch, what is determined is simply that the appliance has moved, rather than an absolute or relative position.

Then, the local policy enforcer checks (62) whether that location meets guidelines of a local policy. A variety of local policies may be utilized in practicing this invention. Examples, given by way of illustration and not exhaustive enumeration, include:

- no motion
- motion over short enough distance that the appliance is likely to still be within the user's house
- previously approved location

If the location meets the local policy, then the local policy enforcer enables (63) the appliance. In various embodiments, enablement may constitute providing power to the functional unit. In other embodiments, enablement may constitute unlocking the functional unit. A suitable dis/enablement mechanism may readily be chosen for a given appliance, given the teachings of this patent. Various mechanisms may be adapted to disable the appliance, to enable the appliance, or to do both; thus the term "dis/enablement". Once the appliance is enabled, the method may end (64) until a next time that, for example, the appliance is powered on, or a next time that it is moved.

If the location does not meet the local policy, then the appliance will communicate information over the communication interface and communication link to the central agency. In various embodiments, the information sent to the central agency may be, for example, the location of the appliance, the fact that the appliance has moved, an indication of in what manner

the local policy was failed, a unique identification of the appliance, an identification of the owner of the appliance, a most recent location which did not fail the local policy, or any combination of such information or other suitable information.

The central agency's remote policy enforcer will make a determination (65) of whether the new location (or other submitted data) meets a remote policy. A variety of remote policies may be utilized in practicing this invention, such as, for example:

- motion over a short enough distance that theft is unlikely
- motion to a pre-approved location such as a repair facility
- motion to a new location authorized by the owner pursuant to a sale of the appliance
- Nth instance of motion where N is less than a predetermined value
- total motion during the lifetime of the appliance is less than a predetermined maximum, such as a prepaid rental mileage
- motion to a location still within a country within which usage of the appliance is permitted by law

If the information, e.g., location meets the remote policy, the central agency remotely enables (66) the appliance. This may be done by sending an enablement signal or value back over the communication link, or by other suitable mechanism. In some instances, it may be desirable to have the appliance be self-enabling unless the central agency disables the appliance. Upon receipt at the communication interface of the dis/enablement signal, the local policy enforcer triggers the dis/enabler to enable or disable the functional unit.

In some embodiments, it may be desirable to update (67) the appliance registry with the new location or other information provided by the appliance or derived from such information.

Once the appliance is enabled and the new information is registered, the method may end (68) until a next time it is utilized.

If the location failed the remote policy, in some embodiments the appliance may simply be disabled (not shown). In other embodiments, it may be more desirable to provide for a mechanism to allow the appliance to be used even though its movement has failed both the local and remote policies. One suitable choice is by authenticating (69) the user. This may involve the user inserting a key into the user authenticator, or the user entering a password into the user authenticator, or the user authenticator gathering biometric data about the user, such as via a thumbprint pad or an iris scan.

If the user is not authenticated, the appliance notifies (70) the central agency, which in turn may notify (71) law enforcement. In some embodiments, the authentication may be checked at the central agency rather than at the appliance; in this case, the appliance will not need to notify (70) the central agency. The central agency may provide to law enforcement any of the data which the central agency has about the user, the location and identity of the appliance, and so forth. In some embodiments, the user authenticator on the appliance may be simply a data input device (whether it be a key, a password, or a biometric input device), and the logic to determine whether the user is authentic may reside at the central agency. This would aid in preventing a thief from altering the output of the user authenticator, or sending back simplistic "he is authentic" types of messages. In such cases, the notification (70) to the central agency will be data to be used in a determination, rather than an outcome of a determination. The method may end (72) with the appliance being left in a disabled state, or in some embodiments, in an enabled state. In some cases, the functionality of the device (such as a defibrillator) is important enough that it is preferable to leave the device functioning in the hands of a possible thief. In

some cases, it may be desirable to leave the device operational so that the thief is unaware that the theft has been noticed and reported to law enforcement. In some embodiments, the law enforcement notification may be done directly by the appliance, rather than, or in addition to, by the central agency.

If the user is authenticated, the appliance is enabled (73), the register is updated (74), and the method ends (75).

In some embodiments, the local policy and/or remote policy may have dynamically adjustable guidelines. Consider the example of a golf cart. The first time the golf cart is turned on, the policies may require a user authentication. Then, as long as the golf cart does not leave the general vicinity (meaning that it is likely to still be at the same golf course), no authentication may be required. Then, when the cart suddenly moves to a different course, authentication may again be required. But then, on a second or third trip to different courses, within the same city, authentication may not be required; the policies may learn that the legitimate user has recently changed his playing habits.

FIG. 3 illustrates another embodiment of a method for practicing the invention. The method begins (80) and the appliance attempts to authenticate (81) the user. If the user is not authenticated, the appliance is disabled (82), law enforcement is notified (83), and the method ends (84). If the user is authenticated, the location of the appliance is determined (84). If the location meets the local policy (86), the appliance is enabled (87) and the new location and so forth may optionally be registered (88), then the method returns to re-checking the location, providing continuous location policy checking. If the location fails the local guidelines, then it is checked against the global guidelines (89). If it meets the local guidelines, the appliance is enabled (90) and the new location and so forth may optionally be registered (91), and the method

returns to re-checking the location continuously. If the remote policy is also failed, the appliance is disabled (92), law enforcement is notified (93), and the method ends (94). Alternatively, the method could disable the appliance at the start, so it would be disabled until one of the policies enables it.

VI. ISSUES

A. Are Claims 1-3, 6-9, 11-20, 31-45 and 47-73 Patentable Under 35 U.S.C. § 103(a) Over Hertel in View of Johnson, et al.?

B. Are Claims 4, 5, 10 and 46 Patentable Under 35 U.S.C. § 103(a) Over Hertel and Johnson, et al. In Combination With Mansell?

VII. GROUPING OF THE CLAIMS

For purposes of this Appeal, Appellants have grouped together Claims as follows:

Group A: Claims 1-3, 6-9, 11-20, 31-45 and 47-73;

Group B: Claims 4, 5, 10 and 46.

VIII. ARGUMENT

A. Claims 1-3, 6-9, 11-20, 31-45 and 47-73 Are Patentable Under 35 U.S.C. § 103(a) Over Hertel in View of Johnson, et al.

In the Final Office Action, Appellants' Claims 1-3, 6-9, 31-45 and 47-73 were rejected under 35 U.S.C. § 103(a) as being unpatentable over United States Patent No. 5,532,690 (Hertel) as applied in combination with United States Patent No. 5,557,254 (Johnson).

Appellants' independent Claims 1, 31, 41, 51, 61 and 65 are respectively directed to an apparatus (Claims 1 and 61), a method (Claims 31, 51 and 65), and a system (Claim 41) in which information is conveyed to "central agency," (or "external agent" or "remote agent device"). That information indicates a failure to comply with a local policy. In one embodiment, the information may be location information of, for example, a vehicle. The failure to comply with local policy may result from a location of the vehicle outside boundaries specified in the local

policy. The central agency, for example, determines whether the information, although noncompliant with local policy, is nonetheless compliant with a "remote" policy. If so, the central agency returns an enable signal so that the apparatus (i.e., vehicle) is enabled.

Because none of the cited references, nor any tenable combination of, or modification to, them disclose or suggest this feature (that is, a technique in which information that is determined to be noncompliant with a local policy is nevertheless determined by a central agency to be compliant with a remote policy), Appellants respectfully submit that independent Claims 1, 31, 41, 51 and 65 are patentable over the cited art.

In pertinent part, the Final Office Action recognizes that Hertel does not disclose transmission of an enable signal by the remote agent in situations where there exists noncompliance with a local policy but there does exist compliance with a remote policy. *See,* e.g., Final Office action at p. 17, line 23-p. 18, line 1. However, the Final Office Action misapprehends Appellant's independent Claims and concludes that Johnson, et al. discloses aspects of Appellants' independent Claims are not present in Hertel. In this regard, it is important to recognize that Appellant's Claims are directed to a technique where, initially, information is detected and determined to be noncompliant with a local policy. That information is then transmitted to a remote agent. If the remote agent determines that the information, which is noncompliant with a local policy, is nonetheless compliant with a remote policy, then the appliance is enabled. Johnson does not disclose this sequence of events, wherein compliance with a remote policy is effective to override noncompliance with a local policy.

As indicated above, the gravamen of Appellants' request fro reversal of the rejections that inhere in the Final Office Action is, simply, that neither Hertel, nor Johnson, et al., nor any sustainable combination of, or modification to, them, discloses or preemption of a local policy by

a remote policy, wherein preemption by the remote policy is based on the same information as was considered by the local policy.

Moreover, the Final Office Action is facially defective in that there is provided no specific identification in the disclosures of either Hertel or Johnson, et al. of either Hertel or Johnson, et al. of the above-referenced aspect of Appellants' Claims. The Final Office Action simply asserts that "the transmitted information includes location information in col. 12 lines 51-55 and the remote policy includes location in col. 11 lines 55-65. Final Office Action at page 3, ll. 13-15. Appellants are unable to perceive, and the Final Office Action flatly fails to reveal, the manner in which the reference passage from Johnson, et al. may be combined with Hertel to under Appellants' Claims unpatentable under 35 U.S.C. § 103(a).

Specifically, in the portion of Johnson that is relied on in Final Office Action, there is described a sequence in which the central agency first receives an "alarm" signal in some form. Subsequent to the transmission of the alarm, authentication information is sent. If the "authentication" is effective, the apparatus (e.g., automobile) is not disabled. Note, however, this process is a marked deviation from Appellant has disclosed and claimed. To reiterate, Appellant discloses and claims a technique where the *same information* (e.g., location) is evaluated for compliance, first with a local policy and, subsequently, with a remote policy. In contradiction, Johnson discloses a technique in which information of one type (authentication) is used to override the effect of information of a second type (alarm).

Accordingly, Appellants respectfully submit that there has been demonstrated in the Final Office Action no tenable combination of, or modification to Hertel and/or Johnson, that discloses or suggest Appellants' the subject matter of Appellants' independent Claims 1, 31, 41, 51, 61

and 65. Therefore, the above-referenced Claims are patentable over the cited art, and reconsideration is in order.

Claims 2, 3, 6, 9, 11-20, 45, 46-50, 52-60, 62-64 and 66-73 depend respectively, from Claims 1, 31, 41, 51, 61 and 65 and are, for at least this reason, likewise patentable over Hertel in view of Johnson, et al.

B. Claims 4, 5, 10 and 46 Are Patentable Under 35 U.S.C. § 103(a) Over Hertel and Johnson, et al. In Combination With Mansell

Appellants' Claims 4, 5, 10, depend from Claim 1 and are, for at least this reason, likewise patentable over the cited art.

Appellants' Claim 46 depends from Claim 41 and is, for at least this reason, likewise patentable over the cited art.

IX. CONCLUSION

Inasmuch as there exists no legally tenable modification to, or combination of, the cited references that discloses or suggests a technique wherein a remote policy operates to preempt a local policy, based on the same information, a *prima facie* case of obviousness has not been made with respect to Appellants' Claims 1-20 and 30-73. Accordingly, the rejection of Appellant's Claims 1-20 and 31-73 is in all respects erroneous, and Appellant respectfully requests that the rejection of the Claims be reversed.

Respectfully submitted,

Date: January 15, 2004

John A. Odozynski
Registration No. 28,769
8554 Katy Fwy, Ste 100
Houston, TX 77024-1805
512/418-9944 [Phone]
713/468-8883 [Facsimile]

APPENDIX OF CLAIMS

The claims on appeal are:

1. An apparatus comprising:

a functional unit;

a location determination device;

a local policy enforcement device coupled to the location determination device and to the functional unit; and

a communication interface coupled to the local policy enforcement device to transmit to a central agency information related to a failure to meet a local policy and to receive from the central agency an enablement signal if the information complies with a remote policy.

2. The apparatus of claim 1 wherein the location determination device comprises a position detection device.

3. The apparatus of claim 2 wherein the position determination device comprises a global positioning system receiver.

4. The apparatus of claim 2 wherein the position determination device comprises an accelerometer.

5. The apparatus of claim 1 wherein the location detection device comprises a motion detection device.

6. The apparatus of claim 1 further comprising:

a user authenticator coupled to the local policy enforcement device.

7. The apparatus of claim 6 wherein the user authenticator comprises a password device.

8. The apparatus of claim 6 wherein the user authenticator comprises a biometric input device.

9. The apparatus of claim 6 wherein the location determination device comprises a global positioning system receiver.

10. The apparatus of claim 6 wherein the location determination device comprises an accelerometer.

11. The apparatus of claim 1 wherein the local policy enforcement device comprises means for determining whether the apparatus is within a distance from a location.

12. The apparatus of claim 11 wherein the distance is a predetermined distance.

13. The apparatus of claim 11 wherein the location is a predetermined location.

14. The apparatus of claim 11 wherein the location is a previously-determined location of the apparatus.

15. The apparatus of claim 14 wherein the distance is a predetermined distance.

16. The apparatus of claim 1 wherein the local policy enforcement device comprises means for dynamically adapting a local policy in response to previous location determinations and previous applications of the local policy.

17. The apparatus of claim 1 wherein the local policy enforcement device comprises means for determining, in response to a determination by the location determination device that the apparatus has been moved to a new location, whether the new location complies with a local policy.

18. The apparatus of claim 17 wherein the local policy is whether the new location is a pre-approved location.

19. The apparatus of claim 17 wherein the local policy is whether the new location is within a distance from a prior location of the apparatus.

20. The apparatus of claim 19 wherein the distance is a predetermined distance.

31. A method of operating an apparatus, the method comprising:

performing authentication of an attempted user of the apparatus;

if the user is determined to be not authorized to use the apparatus,

disabling the apparatus; and

if the user is determined to be authorized to use the apparatus,

determining a location of the apparatus,

checking whether the location complies with a local policy administered by the apparatus,

if the location complies with the local policy,

enabling the apparatus, and

if the location does not comply with the local policy,

inquiring of an external agent whether the location complies with a remote policy administered by the external agent,

if the location complies with the remote policy,

enabling the apparatus, and

if the location does not comply with the remote policy,

disabling the apparatus.

32. The method of claim 31 further comprising:

the remote agent providing an electronic notification to a law enforcement device; and

the remote agent providing an electronic notification to the law enforcement device;

wherein the notifications to the law enforcement device include providing data identifying the location of the apparatus.

33. The method of claim 32 wherein the notifications to the law enforcement device further include providing data gathered during the authentication of the user.

34. The method of claim 33 wherein the data comprises biometric input data.

35. The method of claim 31 further comprising:

the remote agent registering the location of the apparatus.

36. The method of claim 31 wherein the local policy comprises determining whether the location is in compliance with a policy selected from the group comprising:

the location of the apparatus is within a predetermined area;

the location of the apparatus is less than a predetermined distance from a prior location; and

the location of the apparatus is a pre-approved location.

37. The method of claim 31 wherein the local policy comprises determining whether the location is in compliance with a distance-based policy.

38. The method of claim 31 wherein the local policy comprises determining whether the location is in compliance with an area-based policy.

39. The method of claim 31 wherein the remote policy comprises determining whether the location is in compliance with a policy selected from the group comprising:

the location of the apparatus is within a predetermined area;

the location of the apparatus is less than a predetermined distance from a prior location;

the location has been pre-approved by a registered owner of the apparatus;

the location is an authorized repair facility for the apparatus;

all locations have been pre-approved until a first registration at a first location;

total motion of the apparatus since a predetermined time is less than a predetermined cumulative distance;

the apparatus has been moved fewer times than a predetermined number; and

the apparatus is within a non-export-controlled country;.

40. The method of claim 31 further comprising at least one of:

dynamically adjusting the local policy; and

dynamically adjusting the remote policy.

41. A system comprising:

a communication link;

an appliance including,

a functional unit;

a location determination device;

a local policy enforcement device coupled to the communication link and to the location determination device, the local policy enforcement device to transmit to a remote agent device information related to a failure to meet a local policy; and

the remote agent device including,

a registry adapted to store information regarding the apparatus; and

a remote policy enforcement device coupled to the communication link and to the registry, the remote policy enforcement device to transmit to the apparatus an enablement signal if the device information does not meet a local policy but does meet a remote policy.

42. The system of claim 41 wherein the information includes location information.

43. The system of claim 42 wherein the appliance further includes a user authentication device coupled to the local policy enforcement device.

44. The system of claim 43 wherein the information further includes user identification information.

45. The system of claim 41 wherein the location determination device comprises a global positioning system receiver.

46. The system of claim 41 wherein the location determination device comprises an accelerometer.

47. The system of claim 41 wherein the local policy enforcement device comprises means for determining whether the appliance is in a location, determined by the location determination device, which location complies with a policy selected from the group comprising:

the location of the appliance is within a predetermined area;

the location of the appliance is less than a predetermined distance from a prior location; and

the location of the appliance is a pre-approved location.

48. The system of claim 47 wherein the remote policy enforcement device comprises means for determining whether the location complies with a policy selected from the group comprising:

the location of the appliance is within a predetermined area;

the location of the appliance is less than a predetermined distance from a prior location;

the location has been pre-approved by a registered owner of the appliance;

the location is an authorized repair facility for the appliance;

all locations have been pre-approved until a first registration at a first location;

total motion of the appliance since a predetermined time is less than a predetermined cumulative distance;

the appliance has been moved fewer times than a predetermined number; and

the appliance is within a permitted country.

49. The system of claim 41 further comprising:

means for dynamically adjusting a local policy of the local policy enforcement device.

50. The system of claim 41 further comprising:

means for dynamically adjusting a remote policy of the remote policy enforcement device.

51. A method comprising:

determining a location of an apparatus;

the apparatus determining whether the location complies with a local policy;

if the location complies with the local policy,

enabling the apparatus;

if the location does not comply with the local policy,

transmitting to a remote device information related to failure of the apparatus to comply with the local policy;

a remote device determining whether the location complies with a remote policy;

if the location complies with the remote policy,

enabling the apparatus,

if the location does not comply with the remote policy,

disabling the apparatus.

52. The method of claim 51 further comprising, if the location does not comply with the remote policy:

performing authentication of a user of the apparatus; and

if the user is authenticated,

enabling the apparatus.

53. The method of claim 52 further comprising, if the location complies with the remote policy:

the remote device registering information provided from the apparatus to the remote device.

54. The method of claim 53 wherein the information comprises information identifying the location.

55. The method of claim 52 further comprising, if the user is not authenticated:
the remote device sending a notification to a law enforcement device.

56. The method of claim 55 wherein the notification comprises an identification of the location of the apparatus.

57. The method of claim 56 wherein the notification further comprises information gathered during the authentication of the user.

58. The method of claim 57 wherein the information comprises biometric input data.

59. The method of claim 51 further comprising:
the apparatus dynamically adjusting the local policy.

60. The method of claim 59 further comprising:
the remote device dynamically adjusting the remote policy.

61. An apparatus comprising:
a functional unit;
means for disabling the functional unit;
means for identifying a location of the apparatus;
means for communicating with a remote agent; and
means for checking the location against a local policy and for causing the means for disabling to enable the functional unit if the location complies with the local policy and for causing the means for disabling to enable the functional unit if the location does not comply with the local policy and the remote agent indicates that the location does comply with a remote policy.

62. In the apparatus of claim 61, the improvement further comprising:
means for authenticating a user of the apparatus; and

the means for checking further for causing the means for disabling to enable the functional unit if the user is authentic, and for causing the means for disabling to disable the functional unit if the user is not authentic.

63 (canceled)

64. In the apparatus of claim 63, the improvement further comprising:

means for authenticating a user of the apparatus; and

the means for checking further for causing the means for disabling to enable the functional unit if the user is authentic, and for causing the means for disabling to disable the functional unit if the user is not authentic.

65. A method of operating an apparatus, the method comprising:

determining a location of the apparatus;

determining if the location complies with a local policy;

if the location fails to comply with a local policy, transmitting information related to failure to comply with the local policy to a central agency;

receiving enabling information from the central agency if the location complies with a remote policy; and

receiving disabling information from the central agency if the location fails to comply with the remote policy.

66. A method as defined in 65, wherein the information comprises the location of the apparatus.

67. A method as defined in 65, wherein the information comprises the most recent location of the appliance that complied with the local policy.

68. A method as defined in 65, further comprising:

disabling the apparatus in response to receiving disabling information from the central agency.

69. A method as defined in 65, further comprising :

enabling the apparatus in response to receiving disabling information from the central agency, provided that a user is authenticated.

70. A method as defined in 69, wherein the user is authenticated by a password.

71. A method as defined in 69, wherein the user is authenticated by biometric data.

72. A method as defined in 69, wherein the user is authenticated by a key.

73. A method as defined in 65, further comprising:

dynamically adjusting the local policy.